

Some Constacyclic Codes over Finite Chain Rings

Aicha Batoul, Kenza Guenda and T. Aaron Gulliver *

Abstract

For λ an n -th power of a unit in a finite chain ring we prove that λ -constacyclic repeated-root codes over some finite chain rings are equivalent to cyclic codes. This allows us to simplify the structure of some constacyclic codes. We also study the $\alpha + p\beta$ -constacyclic codes of length p^s over the Galois ring $GR(p^e, r)$.

1 Introduction

Constacyclic codes are a generalization of cyclic codes. While the class of simple root constacyclic codes is well known over fields, little is known about repeated root constacyclic codes over fields, and even less about these codes over finite chain rings. Recently, simple root constacyclic codes over finite chain rings and the repeated root cyclic and negacyclic codes over finite fields have been studied [22, 23]. In this work, we generalize the results in [22, 23]. The structure of constacyclic codes over some chain rings is given, as well as conditions on the equivalence between constacyclic codes over finite chain rings and cyclic codes. As a special case, we consider the structure of $(\alpha + \beta p)$ constacyclic codes of length p^s over $GR(p^e, r)$. Besides contributing to what is known concerning this class of codes, our motivation in studying these codes comes from the fact that repeated root cyclic codes contains many optimal codes, and the decoding complexity can be low as shown by Van Lint in the binary case [33] and Byrne et al. [6] for codes over Z_4 . Furthermore, repeated root cyclic codes have found applications in DNA computing [34].

The remainder of this paper is organized as follows. In Section 2, we give some preliminaries results concerning finite chain rings. Section 3 gives conditions on the scalar equivalency between constacyclic codes and cyclic codes over finite fields (for both simple

*A. Batoul and K. Guenda are with the Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algeria. T. A. Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, PO Box 3055, STN CSC, Victoria, BC, Canada V8W 3P6. email: agulliver@ece.uvic.ca.

and repeated roots). In Section 4, we generalize some results of Section 3 to finite chain rings. Finally, the structure of $(\alpha + \beta p)$ -constacyclic codes of length p^s over $GR(p^e, r)$ is considered in Section 5.

2 Preliminaries

A finite chain ring is a finite local, principal commutative ring R with $1 \neq 0$ such that its ideals are ordered by inclusion. Hence if $\langle \gamma \rangle$ is the maximal ideal of the finite chain ring R , then γ is nilpotent with nilpotency index some integer e . The ideals of R form the following chain

$$\langle 0 \rangle = \langle \gamma^e \rangle \subsetneq \langle \gamma^{e-1} \rangle \subsetneq \dots \subsetneq \langle \gamma \rangle \subsetneq R.$$

The simplest examples of finite chain rings are the finite fields. Since they are chain rings with nilpotency index 0, the nilradical of R is $\langle \gamma \rangle$, so all the elements of $\langle \gamma \rangle$ are nilpotent. Therefore the elements of $R \setminus \langle \gamma \rangle$ are units. We denote this group by R^* . Since $\langle \gamma \rangle$ is a maximal ideal, the residue ring $\frac{R}{\langle \gamma \rangle}$ is a field which we denote by K . The natural surjective ring morphism is given by

$$\begin{aligned} \mu : R &\longrightarrow K \\ a &\longmapsto \mu(a) = a + \langle \gamma \rangle \end{aligned} \tag{1}$$

The map given in (1) extends naturally to a map from $R[x] \longrightarrow K[x]$. A polynomial f of $R[x]$ is called basic irreducible if $\mu(f)$ is irreducible in $K[x]$.

Let $|R|$ denote the cardinality of R . If $|K| = q = p^r$ for some integer r , then

$$|R| = |K| \cdot |\langle \gamma \rangle| = |K| \cdot |K|^{e-1} = |K|^e = p^{er}. \tag{2}$$

A code C of length n over R is a subset of R . If the code is a submodule we say that the code is linear. Here, all codes are assumed to be linear.

Lemma 2.1 ([32]) *Let R be a finite commutative chain ring with maximal ideal $\langle \gamma \rangle$, residue field K and nilpotency e . Then the following hold:*

- i) *the distinct proper ideals of R are $\langle \gamma^i \rangle$, $i = 1, 2, \dots, e-1$;*
- ii) *for $i = 1, 2, \dots, e-1$, $|\langle \gamma^i \rangle| = |K|^{e-i}$.*

A special case of finite chain rings are the called Galois rings. The Galois ring $GR(p^e, r)$ is a ring of characteristic p^e and cardinality p^{er} . We have $GR(p^e, 1) = \mathbb{Z}_{p^e}$ and $GR(p, r) = F_{p^r}$. The Galois ring $GR(p^e, r)$ is a local ring with maximal ideal $\langle p \rangle = pGR(p^e, r)$ and residue field $GR(p^e, r)/pGR(p^e, r) = F_{p^r}$. If $f(x) \in \mathbb{Z}_{p^e}[x]$ is a monic basic irreducible polynomial of degree r , then the Galois ring of degree r over \mathbb{Z}_{p^e} is the residue class ring

$$GR(p^e, r) = \mathbb{Z}_{p^e}[x]/(f(x)).$$

If ξ is a root of $f(x)$, then $GR(p^e, r) = \mathbb{Z}_{p^e}[\xi]$, i.e., $GR(p^e, r)$ is a free module of rank r over \mathbb{Z}_{p^e} with $\{1, \xi, \xi^2, \dots, \xi^{r-1}\}$ as a basis. All Galois rings of the same orders are isomorphic.

There exists an element ξ of order $p^r - 1$ in $GR(p^e, r)$ called a primitive element of $GR(p^e, r)$, ξ is a root of a unique monic basic primitive polynomial of degree r over \mathbb{Z}_{p^e} and dividing $x^{p^r-1} - 1$ in $\mathbb{Z}_{p^e}[x]$. If

$$\mathfrak{T}_r = \{0, 1, \xi, \dots, \xi^{p^r-2}\},$$

then each element $a \in GR(p^e, r)$ can be uniquely expressed as

$$a = a_0 + a_1 p + \dots + a_{e-1} p^{e-1}$$

where $a_0, a_1, \dots, a_{e-1} \in \mathfrak{T}_r$. This representation is called the p -adic representation of the elements of the Galois ring $GR(p^e, r)$, and is the generalization of the usual representation of the non-zero elements of a finite field as the powers of a primitive element.

Let R be a finite chain ring. For a given unit $\lambda \in R$, a code C is said to be constacyclic, or more precisely λ -constacyclic, if $(\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$, whenever $(c_0, c_1, \dots, c_{n-1}) \in C$. The cyclic and negacyclic codes are obtained when λ is 1 and -1, respectively. It is well-known that the λ -constacyclic codes over a finite chain ring R are ideals of $R[x]/\langle x^n - \lambda \rangle$.

Two codes are called equivalent if there exists a monomial permutation which send one to another. MacWilliams [27] proved that there exists a monomial permutation between two codes over a finite field if and only if there exists a linear Hamming isometry. Wood [35] extended this result to codes over finite chain rings. Several weights over rings can be defined. A weight on a code C over a finite chain ring is called homogeneous if it satisfies the following assertions.

- (i) $\forall x \in C$ and $\forall u \in R^* : w(x) = w(ux)$
- (ii) There exists a constant $\xi = \xi(w) \in \mathbb{R}$ such that

$$\sum w(x)_{x \in U} = \xi |U|,$$

where U is any subcode of C .

Honold and Nechaev [25] proved that for codes over a finite chain ring there exists a homogeneous weight. A linear morphism $f : R \rightarrow R$ is called a homogeneous isometry if it is a linear homomorphism which preserve the homogeneous weight.

Lemma 2.2 ([21]) *Let R be a finite chain ring, C a linear code over R and $\phi : C \rightarrow R^n$ an embedding. Then the following are equivalent.*

- (i) ϕ is a homogeneous isometry.
- (ii) C and $\phi(C)$ are equivalent.

Here when two codes are said to be equivalent it means that they are monomially equivalent.

Let n be a positive integer and q a prime power. Then we denote by $\text{ord}_n(q)$ the multiplicative order of q modulo n . This is the smallest integer l such that $q^l \equiv 1 \pmod{n}$. The notation $q \equiv \square \pmod{q}$ means that q is a quadratic residue modulo n .

3 Constacyclic Codes over Finite Fields

In this section, we give the structure of repeated root constacyclic codes over finite fields and we give conditions on the existence of an isomorphism between constacyclic and cyclic codes. We begin with the following lemma.

Lemma 3.1 *Let α be a primitive element of \mathbb{F}_q , $q = p^r$ and $\lambda = \alpha^i$ for $i \leq q - 1$. Then the following holds:*

- (i) $x^n = \lambda$ has a solution in \mathbb{F}_q if and only if $(n, q - 1) | i$;
- (ii) if $n = 2m$ is an oddly even integer and q is an odd prime power, then $x^n = -1$ has a solution in \mathbb{F}_q^* if and only if $-1 \equiv \square \pmod{q}$;
- (iii) $-1 \equiv \square \pmod{q}$ if and only if $p \equiv 1 \pmod{4}$, r any integer, or $p \equiv 3 \pmod{4}$ and r even.

Proof. For the Part (i), assume that $x^n = \lambda$ has a solution in \mathbb{F}_q . Then this solution is equal to $\gamma = \alpha^j$ for some j and satisfies $(\alpha^j)^n = \alpha^i$. This is equivalent to $\alpha^{nj-i} = 1$. Since the order of α is $q - 1$, then $(q - 1) | nj - i \Leftrightarrow nj - r(q - 1) = i$ for some integer r . This gives that $(n, q - 1) | i$.

Assuming the existence of a solution α^i of $x^n = -1$, then from Part (i) we have that $(n, q - 1) | i$. If n is even and q is odd then $(n, q - 1)$ is even, hence i is even. This gives that $-1 = \square \pmod{q}$. Conversely, assume that $-1 \equiv \square \pmod{q}$. Then there exists an even $i = 2i'$ such that $-1 = \alpha^i$. Since $n = 2m$ is oddly even, $(-1)^m = -1 = \alpha^{2mi'} = (\alpha^{i'})^n$, and hence there exists a solution of $x^n + 1 = 0$ in \mathbb{F}_{q^r} .

For Part (iii), we have that $-1 \equiv \square \pmod{q}$ if and only if $(-1)^{\frac{p^r-1}{2}} = 1 \pmod{q}$ [26, Lemma 6.2.4]. This is equivalent to $p^r \equiv 1 \pmod{4}$, which can happen if and only if $q \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{4}$, r any integer, or $p \equiv 3 \pmod{4}$ and r even. \square

Proposition 3.2 *Let q be a prime power, n a positive integer and $\lambda \in \mathbb{F}_q^*$. If \mathbb{F}_q^* contains an n -th root δ of λ , then a λ -constacyclic code of length n is equivalent to a cyclic code of length n .*

Proof. Let $\delta \in \mathbb{F}_q^*$ such that $\delta^n = \lambda$ and define

$$\begin{aligned} \phi: \mathbb{F}_q[x]/(x^n - 1) &\longrightarrow \mathbb{F}_q[x]/(x^n - \lambda) \\ f(x) &\longmapsto \phi(f(x)) = f(\delta^{-1}x) \end{aligned}$$

It is obvious that ϕ is a ring homomorphism and is Hamming weight preserving. Hence we only need prove that ϕ is a one-to-one map. For this, let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}_q[x]$ such that $f(x) \equiv g(x) \pmod{x^n - 1}$. This is equivalent to the existence of $h(x) \in \mathbb{F}_q[x]$ such that $f(x) - g(x) = h(x)(x^n - 1)$. This equality is true if and only if $f(\delta^{-1}x) - g(\delta^{-1}x) = h(\delta^{-1}x)[(\delta^{-1}x)^n - 1]$ is true. We have that $h(\delta^{-1}x)[\delta^{-n}x^n - 1] = \delta^{-n}h(\delta^{-1}x)[x^n - \delta^n] = \delta^{-n}h(\delta^{-1}x)[x^n - \lambda]$, so for $f, g \in \mathbb{F}_q[x]/(x^n - 1)$

$$\phi(f(x)) = \phi(g(x)) \iff g(x) = f(x).$$

Then ϕ is well defined and one-to-one, and hence is a ring isomorphism and a Hamming isometry. Since the λ -constacyclic and cyclic codes are ideals, the result follows from [27]. \square

Corollary 3.3 *Let $q = p^r$ be a prime power, n a positive integer and $\lambda \in \mathbb{F}_q^*$. If \mathbb{F}_q^* contains an n -th root δ of λ and the f_i , $1 \leq i \leq r$, are the monic irreducible factors of $x^n - 1$ in \mathbb{F}_q , then $x^n - \lambda = \lambda \prod_{i=1}^r f_i(\delta^{-1}x)$ is the factorization of $x^n - \lambda$ into irreducible factors over \mathbb{F}_q .*

Proof. Assume that $x^n - 1 = \prod_{i=1}^r f_i(x)$ is the factorization of $x^n - 1$ into irreducible factors over \mathbb{F}_q . This factorization is unique since it is over a unique factorization domain (UFD), but in this case $(n, p) \neq 1$, so the factors are not necessarily coprime. Since ϕ is a ring isomorphism, $\phi(x^n - 1) = \delta^{-n}x^n - 1 = \delta^{-n}(x^n - \lambda) = \prod_{i=1}^r \phi(f_i(x)) = \prod_{i=1}^r f_i(\delta^{-1}x)$, as the image of 0 by ϕ is 0. \square

Theorem 3.4 *Let F_q be a finite field, $q = p^r$ a prime power, and n an integer such that $(n, q - 1) = 1$. Then all constacyclic codes of length n over F_q are equivalent to cyclic codes of length n over F_q .*

Proof. Let α be a primitive element of \mathbb{F}_q and $\lambda \in \mathbb{F}_q^*$. Then there exists an integer i such that $\lambda = \alpha^i$. Since $(n, q - 1) = 1$, then $(n, q - 1) | i$ and by Lemma 3.1 there exists $\delta \in \mathbb{F}_q^*$ such that $\delta^n = \lambda$. By Proposition 3.2, the λ -constacyclic codes of length n over \mathbb{F}_q are equivalent to cyclic codes of length n over \mathbb{F}_q . \square

Example 3.5 *Let \mathbb{F}_q be a finite field, $q = p^r$ a prime power, and $n = mp^s$ an integer such that $(m, p^r - 1) = 1$. Then all constacyclic codes of length n over \mathbb{F}_q are equivalent to cyclic codes of length n over \mathbb{F}_q .*

Theorem 3.6 *Let \mathbb{F}_q be a finite field, $q = p^r$ an odd prime power, and m an odd integer such that $(m, p) = 1$. Let $\lambda \in \mathbb{F}_q^*$ such that there exists $\delta \in \mathbb{F}_q^*$ and $\delta^m = \lambda$. Then the following hold:*

- (i) $\pm\lambda$ -constacyclic codes of length mp^s over \mathbb{F}_q are equivalent to cyclic codes over \mathbb{F}_q ;
- (ii) If $q \equiv 1 \pmod{4}$ and $\delta = \beta^2$ in \mathbb{F}_q , then $\pm\lambda$ -constacyclic codes of length $2mp^s$ over \mathbb{F}_q are equivalent to cyclic codes over \mathbb{F}_q .

Proof.

- i) Let $\lambda \in \mathbb{F}_q^*$ such that there exists $\delta \in \mathbb{F}_q^*$ and $\delta^m = \lambda$. Then exists $\alpha \in \mathbb{F}_q^*$ such that $\alpha^{p^s} = \delta$, so that $\lambda = \delta^m = \alpha^{mp^s}$. Since mp^s is odd, we obtain $-\lambda = (-\delta)^m = (-\alpha)^{mp^s}$, and the result follows by Proposition 3.2.
- ii) Let $\lambda \in \mathbb{F}_q^*$ such that there exists $\beta \in \mathbb{F}_q^*$ and $\beta^{2m} = \lambda$. Then there exists $\rho \in \mathbb{F}_q^*$ so that $\rho^{p^s} = \beta$ and $\lambda = \beta^{2m} = \rho^{2mp^s}$. Thus ρ is a $2mp^s$ -th root of λ in \mathbb{F}_q . If $q \equiv 1 \pmod{4}$, by Lemma 3.1 there exists $\xi \in \mathbb{F}_q$ such that $\xi^2 = -1$. Then $-\lambda = (-1)^{mp^s} \beta^{2m} = \xi^{2mp^s} \rho^{2mp^s} = (\xi\rho)^{2mp^s}$, and $\xi\rho$ is a $2mp^s$ -th root of $-\lambda$ in \mathbb{F}_q . The result then follows by Proposition 3.2.

□

Example 3.7 When m is odd we have $(-1)^m = -1$. Then from Part (i) of Theorem 3.6, the negacyclic codes of length mp^r are equivalent to cyclic codes.

When m is odd, $q \equiv 1 \pmod{4}$, and $q = p^r$ an odd prime power, from Part (ii) of Theorem 3.6 the negacyclic codes of length $2mp^s$ are equivalent to cyclic codes of length $2mp^s$ over \mathbb{F}_q . The structure of these codes was also given in [23], and they are generated by

$$\prod_{i=1}^{k_1} f_i(\beta x)^{\alpha_i} \prod_{i=1}^{k_2} f_i(-\beta x)^{\gamma_i},$$

where $k_1, k_2 \leq l$, $\alpha_i, \gamma_i \leq p^s$, $\prod_{i=1}^l f_i(x)$ is the factorization of $x^m - 1$ into monic irreducible factors over $\mathbb{F}_q[x]$, and $\beta^2 = -1$. When $m = 1$, these codes are generated by $\langle (x+\beta)^i(x-\beta)^j \rangle$ $0 \leq i, j \leq p^s$. These codes have also been studied by Dinh [16].

Example 3.8 Let α be a primitive element of \mathbb{F}_{27}^* and $n = 90 = 2 \cdot 5 \cdot 3^2$. Further, let $\lambda \in \{\alpha^{2i}, 1 \leq i \leq 13\}$, and since $(5, 26) = 1$, $\alpha^{2i} = \alpha^{2i(26-5 \cdot 5)} = (\alpha^{-5i})^{2 \cdot 5}$. Then $\beta = \alpha^{-5i}$, $\beta^{27} = (\beta^3)^9$ and $\rho = \beta^3$, so $\lambda = (\alpha^{-15})^{2 \cdot 5 \cdot 9i} = (\alpha^{11})^{2 \cdot 5 \cdot 9i}$. We have $x^{90} - 1 = (x^{10} - 1)^9 = (x^5 - 1)^9(x^5 + 1)^9 = (x - 1)^9(x^4 + x^3 + x^2 + x + 1)^9(x + 1)^9(x^4 - x^3 + x^2 - x + 1)^9$. Since cyclic codes of length 90 over \mathbb{F}_{27} are principal ideals of $\frac{\mathbb{F}_{27}[x]}{x^{90}-1}$, these codes are generated by polynomial of the following form

$$\begin{aligned} & (x - 1)^s(x^4 + x^3 + x^2 + x + 1)^j(x + 1)^k(x^4 - x^3 + x^2 - x + 1)^l \\ & = f_1^s(x)f_2^j(x)f_1^k(-x)f_2^l(-x), \text{ for } s, j, k, l \in \{0, \dots, 9\}. \end{aligned}$$

Therefore λ -constacyclic codes of length 90 over \mathbb{F}_{27} are ideals of $\frac{\mathbb{F}_{27}[x]}{x^{90}-\lambda}$ which is a principal ideal ring, and these codes are generated by

$$\langle f_1^s(\alpha^{-11i}x)f_2^j(\alpha^{-11i}x)f_1^k(-\alpha^{-11i}x)f_2^l(-\alpha^{-11i}x) \rangle, \quad s, j, k, l \in \{0, \dots, 9\}, 1 \leq i \leq 13.$$

The set of all possible generators of λ -Constacyclic codes of length 90 over \mathbb{F}_{27} are given in Table 1.

Table 1: All Possible Generators of λ -Constacyclic Codes of length 90 over \mathbb{F}_{27}

$\lambda = \alpha^{11.i.2.5.9}$	$f_1^s(\alpha^{-11i}x)f_2^j(\alpha^{-11i}x)f_1^k(-\alpha^{-11i}x)f_2^l(-\alpha^{-11i}x)$
$\alpha^{11.2.5.9}$	$\langle f_1^s(\alpha^{-11}x)f_2^j(\alpha^{-11}x)f_1^k(-\alpha^{-11}x)f_2^l(-\alpha^{-11}x) \rangle$
$\alpha^{11.2.2.5.9}$	$f_1^s(\alpha^{-11.2}x)f_2^j(\alpha^{-11.2}x)f_1^k(-\alpha^{-11.2}x)f_2^l(-\alpha^{-11.2}x)$
$\alpha^{11.3.2.5.9}$	$f_1^s(\alpha^{-11.3}x)f_2^j(\alpha^{-11.3}x)f_1^k(-\alpha^{-11.3}x)f_2^l(-\alpha^{-11.3}x)$
$\alpha^{11.4.2.5.9}$	$f_1^s(\alpha^{-11.4}x)f_2^j(\alpha^{-11.4}x)f_1^k(-\alpha^{-11.4}x)f_2^l(-\alpha^{-11.4}x)$
$\alpha^{11.5.2.5.9}$	$f_1^s(\alpha^{-11.5}x)f_2^j(\alpha^{-11.5}x)f_1^k(-\alpha^{-11.5}x)f_2^l(-\alpha^{-11.5}x)$
$\alpha^{11.6.2.5.9}$	$f_1^s(\alpha^{-11.6}x)f_2^j(\alpha^{-11.6}x)f_1^k(-\alpha^{-11.6}x)f_2^l(-\alpha^{-11.6}x)$
$\alpha^{11.7.2.5.9}$	$f_1^s(\alpha^{-11.7}x)f_2^j(\alpha^{-11.7}x)f_1^k(-\alpha^{-11.7}x)f_2^l(-\alpha^{-11.7}x)$
$\alpha^{11.8.2.5.9}$	$f_1^s(\alpha^{-11.8}x)f_2^j(\alpha^{-11.8}x)f_1^k(-\alpha^{-11.8}x)f_2^l(-\alpha^{-11.8}x)$
$\alpha^{11.9.2.5.9}$	$f_1^s(\alpha^{-11.9}x)f_2^j(\alpha^{-11.9}x)f_1^k(-\alpha^{-11.9}x)f_2^l(-\alpha^{-11.9}x)$
$\alpha^{11.10.2.5.9}$	$f_1^s(\alpha^{-11.10}x)f_2^j(\alpha^{-11.10}x)f_1^k(-\alpha^{-11.10}x)f_2^l(-\alpha^{-11.10}x)$
$\alpha^{11.11.2.5.9}$	$f_1^s(\alpha^{-11.11}x)f_2^j(\alpha^{-11.11}x)f_1^k(-\alpha^{-11.11}x)f_2^l(-\alpha^{-11.11}x)$
$\alpha^{11.12.2.5.9}$	$f_1^s(\alpha^{-11.12}x)f_2^j(\alpha^{-11.12}x)f_1^k(-\alpha^{-11.12}x)f_2^l(-\alpha^{-11.12}x)$
$\alpha^{11.13.2.5.9}$	$f_1^s(\alpha^{-11.13}x)f_2^j(\alpha^{-11.13}x)f_1^k(-\alpha^{-11.13}x)f_2^l(-\alpha^{-11.13}x)$

4 Constacyclic Codes over Finite Chain Rings

The purpose of this section is to provide an isomorphism between constacyclic and cyclic codes in a more general setting than those given in [5]. This allows us to simplify the structure of constacyclic codes. To achieve this goal, we extend some results given in the previous section to finite chain rings with characteristic p such that $(n, p) = 1$. For $\lambda \in R^*$, if there exists $\delta \in R^*$ such that $\delta^n = \lambda$, then δ is called an n -th root of λ in R .

Since $R^* = R \setminus \langle \gamma \rangle$, then for all $a \in R^*$ we have $\mu(a) \neq 0$. Further, as the map μ is a surjective homomorphism, it induces the surjective homomorphism $\tilde{\mu} : R^* \longrightarrow \mathbb{F}_q^*$. The following lemma provides the link between the n -th root of elements in R and the n -th root of their images in \mathbb{F}_q .

Lemma 4.1 ([28, p. 355]) *With the notation given above, $\text{Ker}(\tilde{\mu})$ is a p -group.*

We now generalize a result of Dougherty et al. [19, Lemma 4.2].

Proposition 4.2 *Let R be a finite chain ring with residue field \mathbb{F}_{p^r} and n an integer such that $(p, n) = 1$. Further, let $\lambda \in R$ such that $\mu(\lambda) \neq 0$. Then there exists an n -th root of λ in R if and only if there exists an n -th root of $\mu(\lambda)$ in \mathbb{F}_q^* .*

Proof. We first prove that the following map is an automorphism $\xi : Ker(\tilde{\mu}) \rightarrow Ker(\tilde{\mu}), x \mapsto x^n$. Suppose $x, y \in Ker(\tilde{\mu})$ are such that $x^n = y^n$, then $(xy^{-1})^n = 1$. From Lemma 4.1, we have that $Ker(\tilde{\mu})$ is a p -group, and since $(n, p) = 1$ we obtain that $xy^{-1} = 1$. Hence $x = y$, which implies that ξ is a bijection. It is easy to check that ξ is a homomorphism, and hence an automorphism. Let $\lambda \in R$ with $\mu(\lambda) \neq 0$, and suppose $\exists \delta \in R$ such that $\delta^n = \lambda$. Then since μ is a homomorphism, we have $\mu(\delta^n) = \mu(\lambda) \implies \mu(\lambda) = (\mu(\delta))^n$. Now let $c_1 \in \mathbb{F}_{p^r}^*$ such that there exists $\delta_1 \in \mathbb{F}_{p^r}^*$ which satisfies $c_1 = \delta_1^n$. Then there exists $c_0 \in R^*$ and $\delta_0 \in R^*$ such that $\mu(c_0) = c_1$ and $\mu(\delta_0) = \delta_1$. Therefore $\mu(c_0) = \mu(\delta_0^n)$, so then $c_0 \delta_0^{-n} \in Ker(\tilde{\mu})$. Since we already have that ξ is a bijection, there exists $b \in Ker(\tilde{\mu})$ such that $c_0 \delta_0^{-n} = b^n$. Then $c_0 = \delta_0^n b^n = (\delta_0 b)^n$, $\delta_0 b \in R^*$. This implies that $\delta_0 b$ is a n -th root of c_0 in R^* . \square

Theorem 4.3 *Let R be a finite chain ring with residue field \mathbb{F}_q , and let n be an integer such that $(n, q) = 1$. If there exists $\lambda \in F_q^*$ such that $\exists \delta \in \mathbb{F}_q^*$ with $\delta^n = \lambda$, then $\exists \lambda_0$ a unit in R such that $\lambda_0 = \delta_0^n$ and $\mu(\lambda_0) = \lambda$. Further, the λ_0 -constacyclic code of length n over R is equivalent to a cyclic code of length n over R .*

Conversely, if there exists a unit $\lambda \in R$ such that there exists a unit $\delta \in R$ with $\delta^n = \lambda$, then a $\mu(\lambda)$ -constacyclic code of length n over \mathbb{F}_q is equivalent to a cyclic code of length n over \mathbb{F}_q .

Proof. Let R be a finite chain ring with residue field \mathbb{F}_q , and let n be an integer such that $(n, q) = 1$. If there exists $\lambda \in F_q^*$ such that $\exists \delta \in \mathbb{F}_q^*$ with $\delta^n = \lambda$, then by Proposition 4.2 there exists $\lambda_0, \delta_0 \in R^*$ such that $\mu(\lambda_0) = \lambda$ and $\delta_0^n = \lambda_0$. Let

$$\begin{aligned} \psi: R[x]/(x^n - 1) &\longrightarrow R[x]/(x^n - \lambda_0) \\ f(x) &\longmapsto \mu(f(x)) = f(\delta_0^{-1}x). \end{aligned} \tag{3}$$

We need to prove that ψ is an isometry according to a homogeneous weight over R . Let $w(\cdot)$ be a homogeneous weight over R and let $f(x) = a_0 + a_1x + \dots + a_nx^n$ be a codeword in $R[x]/(x^n - 1)$. Then $\psi(f(x)) = a_0 + a_1\delta^{-1}x + a_2\delta^{-1}x^2 + \dots + \delta^{-1}x^n$. Since δ is a unit, it must be that $w(\delta^{-i}a_i) = w(a_i)$, hence $w(\psi(f(x))) = w(f(x))$. By a proof similar to that of Proposition 3.2 for fields, ψ is a ring isomorphism so A is an ideal of $R[x]/(x^n - 1)$. Then $\psi(A)$ is an ideal of $R[x]/(x^n - \lambda_0)$ and if B is an ideal of $R[x]/(x^n - \lambda_0)$, $\psi^{-1}(B)$ is an ideal of $R[x]/(x^n - 1)$. Hence from Lemma 2.2 the result follows.

Conversely, if there exists a unit $\lambda \in R$ such that there exists a unit $\delta \in R$ with $\delta^n = \lambda$, then by Proposition 4.2 $\mu(\lambda) = \mu(\delta)^n$ in F_q . From Proposition 3.2, we deduce that a $\mu(\lambda)$ -constacyclic code of length n over \mathbb{F}_q is equivalent to a cyclic code of length n over \mathbb{F}_q . \square

Corollary 4.4 *Let R be a finite chain ring with residue field F_q with $q = p^r$ a prime power and n a positive integer such that $(n, p) = 1$. In addition, let λ be a unit in R . Then if R contains an n -th root δ of λ and the f_i , $1 \leq i \leq r$ are the monic basic irreducible pairwise coprime factors of $x^n - 1$ in $R[x]$, $x^n - \lambda = \lambda \prod_{i=1}^r f_i(\delta^{-1}x)$ is the factorization of $x^n - \lambda$ into basic irreducible pairwise coprime factors in $R[x]$.*

Proof. Assume that $x^n - 1 = \prod_{i=1}^r f_i(x)$ is the unique factorization of $x^n - 1$ into monic basic irreducible pairwise coprime factors over R . This factorization is unique since $x^n - 1$ is monic, $(n, p) = 1$ and it is over a finite chain ring. Since μ is a ring homomorphism, $\mu(x^n - 1) = \prod_{i=1}^r \mu(f_i)(x)$ is the unique factorization of $\mu(x^n - 1)$ into monic irreducible pairwise coprime factors over F_q . By Corollary 3.3, $x^n - \mu(\lambda) = \mu(\lambda) \prod_{i=1}^r \mu(f_i)(\mu(\delta)^{-1}x)$ is the unique factorization of $x^n - \mu(\lambda)$ into irreducible pairwise coprime over F_q .

From Theorem 4.3, ψ is a ring isomorphism, so $\psi(x^n - 1) = \delta^{-n}x^n - 1 = \delta^{-n}(x^n - \lambda) = \prod_{i=1}^r \psi(f_i(x)) = \prod_{i=1}^r f_i(\delta^{-1}x)$, and $\lambda \prod_{i=1}^r f_i(\delta^{-1}x)$ is a factorization of $x^n - \lambda$ over R . Then $\mu(x^n - \lambda) = \mu(\prod_{i=1}^r f_i(\delta^{-1}x)) = \prod_{i=1}^r \mu(f_i)(\delta^{-1}x) = \prod_{i=1}^r \mu(f_i)(\mu(\delta)^{-1}x)$, $f_i(\delta^{-1}x)$ is basic irreducible over R for $1 \leq i \leq r$ \square

Corollary 4.5 *Let R be a chain ring with maximal ideal $\langle \gamma \rangle$, index of nilpotency e , and residue field \mathbb{F}_q with $q = p^r$ a prime power. Further, let n be an integer such that $(n, q) = 1$ and $\lambda \in 1 + \langle \gamma \rangle$. Then λ -constacyclic codes over R of length n are equivalent to cyclic codes of length n over R .*

Proof. Let $\lambda \in 1 + \langle \gamma \rangle$ so that $\mu(\lambda) = 1$. Then from Proposition 4.2, there exists an n -th root of λ in R since there is an n -th root of 1 in \mathbb{F}_q . Hence from Theorem 4.3, we have that these constacyclic codes are equivalent to cyclic codes. \square

Example 4.6 *If n is an integer such that $(n, q) = 1$ and $\lambda = 1 \pm \gamma^{e-1}$, then λ -constacyclic codes over R of length n are equivalent to cyclic codes of length n over R .*

Corollary 4.7 *Let R be a finite chain ring with residue field \mathbb{F}_{p^r} , $n = 2m$ an oddly even integer and p an odd prime such that $(n, p) = 1$. Then if $p \equiv 1 \pmod{4}$, r an integer, or $p \equiv 3 \pmod{4}$, r even, negacyclic codes of length n over R are equivalent to cyclic codes of length n over R .*

Proof. From Lemma 3.1, if n is oddly even and $p \equiv 1 \pmod{4}$, r an integer, or $p \equiv 3 \pmod{4}$, r even, then $x^n + 1$ has a solution in \mathbb{F}_{p^r} . Hence from Theorem 4.3 the negacyclic codes are equivalent to cyclic codes over R . \square

Next the structure of negacyclic codes of length $2m$ are examined under the assumptions of Corollary 4.7.

Proposition 4.8 *With the assumptions of Corollary 4.7, any cyclic or negacyclic code over R of length $2m$, m odd, over R is a direct sum of two cyclic codes of length m over R .*

Proof. Let $n = 2m$ with m an odd integer and $p \equiv 1 \pmod{4}$, r an integer, or $p \equiv 3 \pmod{4}$, r even, by Lemma 3.1 there exists $\nu \in F_q^*$ such that $\nu^2 = -1$. Then since p is odd and $(p, 2) = 1$, by Proposition 4.2 there exists a unit $\nu_0 \in R$ such that $\nu_0^2 = -1$ in R . Thus $-1 = (-1)^m = (\nu_0^2)^m = (\nu_0)^{2m} = \nu_0^n$. From Theorem 4.3 we deduce that negacyclic codes of length n are equivalent to cyclic codes of length n over R . Since m is odd, then $\frac{R[x]}{x^{2m}-1} \simeq \frac{R[x]}{x^m-1}$. Hence we have

$$\frac{R[x]}{x^{2m}-1} \simeq \frac{R[x]}{x^m-1} \oplus \frac{R[x]}{x^m-1}.$$

\square

Example 4.9 *Let $R = \mathbb{Z}_{25}$ and $n = 18 = 2 \cdot 9$. Since $x^{18} - 1 = (x^9 - 1)(x^9 + 1)$, then*

$$\frac{\mathbb{Z}_{25}[x]}{x^{18}-1} \simeq \frac{\mathbb{Z}_{25}[x]}{x^9-1} \oplus \frac{\mathbb{Z}_{25}[x]}{x^9+1}.$$

In $\mathbb{Z}_{25}[x]$ we have the factorization $x^9 - 1 = (x + 24)(x^2 + x + 1)(x^6 + x^3 + 1)$. Denote the monic basic irreducible factors of $x^9 - 1$ as

$$f_0(x) = (x + 24), f_1(x) = (x^2 + x + 1), \text{ and } f_2(x) = (x^6 + x^3 + 1).$$

Then

$$x^{18} - 1 = (x^9 - 1)(x^9 + 1) = f_0(x)f_1(x)f_2(x)f_0(-x)f_1(-x)f_2(-x)$$

is the factorization of $x^{18} - 1$ in $\mathbb{Z}_{25}[x]$ into monic basic irreducible factors. Then

$$C_1 = \langle f_0(x)f_2(x), 5f_0(x)f_1(x) \rangle$$

and

$$C_2 = \langle f_0(x)f_1(x), 5f_1(x)f_2(x) \rangle$$

generate cyclic codes of length 9 over \mathbb{Z}_{25} . Since 9 is odd, $\frac{\mathbb{Z}_{25}[x]}{x^9-1} \simeq \frac{\mathbb{Z}_{25}[x]}{x^9+1}$, and the image of C_2 is $\langle f_0(-x)f_1(-x), 5f_1(-x)f_2(-x) \rangle$. Then

$$\langle f_0(x)f_2(x), 5f_0(x)f_1(x) \rangle \oplus \langle f_0(-x)f_1(-x), 5f_1(-x)f_2(-x) \rangle$$

is a cyclic code of length 18 over \mathbb{Z}_{25} .

We know that negacyclic codes over \mathbb{Z}_{25} of length 18 are principal ideals of $\frac{\mathbb{Z}_{25}[x]}{x^{18}+1}$. In \mathbb{Z}_{25} , $7^2 = -1$ so $x^{18} + 1 = x^{18} - (-1) = x^{18} - 7^2 = x^9 - 7)(x^9 + 7) = (x^9 - 7^9)(x^9 + 7^9) = 7((-7x)^9 - 1)7((7x)^9 + 1) = -((-7x)^9 - 1)((7x)^9 + 1)$. Since $x^9 - 1 = f_0(x)f_1(x)f_2(x)$, $f_0(-7x)f_1(-7x)f_2(-7x)$ is the factorization of $((-7x)^9 - 1)$ into monic basic irreducible factors in $\mathbb{Z}_{25}[x]$, and $f_0(7x)f_1(7x)f_2(7x)$ is the factorization of $((7x)^9 + 1)$ into monic basic irreducible factors in $\mathbb{Z}_{25}[x]$. We then have

$$\frac{\mathbb{Z}_{25}[x]}{x^{18}+1} \simeq \frac{\mathbb{Z}_{25}[x]}{(-7x)^9-1} \oplus \frac{\mathbb{Z}_{25}[x]}{(7x)^9+1}. \quad (4)$$

Since $\frac{\mathbb{Z}_{25}[x]}{(7x)^9-1} \simeq \frac{\mathbb{Z}_{25}[x]}{(7x)^9+1}$, then for example

$$\langle f_0(7x)f_2(7x), 5f_0(7x)f_1(7x) \rangle \oplus \langle f_0(-7x)f_1(-7x), 5f_1(-7x)f_2(-7x) \rangle$$

is a negacyclic code of length 18 over \mathbb{Z}_{25} .

5 $(\alpha + \beta p)$ -Constacyclic Codes of Length p^s over Finite Galois Rings

Let $R = GR(p^e, r)$ be the finite Galois ring with residue field \mathbb{F}_{p^r} , maximal ideal $\langle p \rangle$, and nilpotency index e . Let α, β be units in R , $n = p^s$, and $\mathcal{R}(\alpha, \beta) = \frac{R[x]}{(x^{p^s} - (\alpha + \beta p))}$. Then the $(\alpha + \beta p)$ -constacyclic codes of length p^s over R are precisely the ideals of $\mathcal{R}(\alpha, \beta)$.

Each element of $GR(p^e, r)$ can be uniquely written as

$$a = a_0 + a_1p + a_2p^2 + \cdots + a_{e-1}p^{e-1}$$

with $a_i \in \mathcal{T}$. Note that \mathcal{T} is equivalent to F_{p^r} . We have $\mu(a) = a_0$, where μ is the map given by (1).

Lemma 5.1 *Let R be a finite commutative ring with identity, and let $x, y \in R$. If $x - y$ is nilpotent in R , then x is a unit if and only if y is a unit.*

Proof. Let $z = x - y$. Since the set of nilpotent element of R is a subgroup in R , if z is nilpotent then x is nilpotent if and only if y is nilpotent. \square

Lemma 5.2 *Assume there exists a unit $\alpha_0 \in R$ such that $\alpha_0^{p^s} = \alpha$. Then in $\mathcal{R}(\alpha, \beta)$ we have $(\alpha_0^{-1}x - 1)^{p^s} = p\rho(x)$ where $\rho(x)$ is a unit in $\mathcal{R}(\alpha, \beta)$. Moreover, the nilpotency index of $(\alpha_0^{-1}x - 1)^{p^s}$ is ep^s .*

Proof. In $\mathcal{R}(\alpha, \beta)$ we have

$$\begin{aligned}
(\alpha_0^{-1}x - 1)^{p^s} &= (\alpha_0^{-1}x)^{p^s} + (-1)^{p^s} + \sum_{i=1}^{p^s-1} (-1)^i \binom{p^s}{i} (\alpha_0^{-1}x)^{p^s-i} \\
&= \alpha_0^{-p^s} x^{p^s} + (-1)^{p^s} + \sum_{i=1}^{p^s-1} (-1)^i \binom{p^s}{i} (\alpha_0^{-1}x)^{p^s-i} \\
&= \alpha^{-1}(\alpha + \beta\gamma) + (-1)^{p^s} + \sum_{i=1}^{p^s-1} (-1)^i \binom{p^s}{i} (\alpha_0^{-1}x)^{p^s-i} \\
&= 1 + (-1)^{p^s} + \alpha^{-1}\beta p + \sum_{i=1}^{p^s-1} (-1)^i \binom{p^s}{i} (\alpha_0^{-1}x)^{p^s-i}
\end{aligned}$$

Let $g(x) = \sum_{i=1}^{p^s-1} (-1)^i \binom{p^s}{i} (\alpha_0^{-1}x)^{p^s-i}$. Expanding $g(x)$ in $(\alpha_0^{-1}x - 1)$ gives

$$\begin{aligned}
g(x) &= \sum_{i=1}^{p^s-1} (-1)^i \binom{p^s}{i} ((\alpha_0^{-1}x - 1) + 1)^{p^s-i} \\
&= \sum_{i=1}^{p^s-1} \sum_{j=0}^{p^s-i} (-1)^i \binom{p^s}{i} \binom{p^s-i}{j} (\alpha_0^{-1}x - 1)^{p^s-i-j},
\end{aligned}$$

where the constant term is

$$g(\alpha_0) = (-1) - (-1)^{p^s}.$$

Hence $g(x)$ can be represented as $g(\alpha_0) + p \sum_{i=1}^{p^s-1} b_i (\alpha_0^{-1}x - 1)^i$ where $b_i \in R$ for $0 \leq i \leq p^s - 1$. Then we have $(\alpha_0^{-1}x - 1)^{p^s} = p\rho(x)$, where

$$\rho(x) = \alpha^{-1}\beta + \sum_{i=1}^{p^s-1} b_i (\alpha_0^{-1}x - 1)^i.$$

From Lemma 5.3, we have that $\rho(x)$ is a unit in $\mathcal{R}(\alpha, \beta)$ since $\alpha^{-1}\beta$ is a unit in R . Hence $(\alpha_0^{-1}x - 1)^{p^s} = 0$ in $\mathcal{R}(\alpha, \beta)$, which means that the nilpotency index of $(\alpha_0^{-1}x - 1)$ is ep^s . \square

Lemma 5.3 *Assume there exists a unit $\alpha_0 \in R$ such that $\alpha_0^{p^s} = \alpha$. Then for $f(x) \in \mathcal{R}(\alpha, \beta)$ the following hold:*

(i) $f(x)$ can be uniquely written as

$$f(x) = a_0 + a_1(\alpha_0^{-1}x - 1) + a_2(\alpha_0^{-1}x - 1)^2 + \cdots + a_{p^s-1}(\alpha_0^{-1}x - 1)^{p^s-1}$$

where $a_i \in R, 0 \leq i \leq p^s - 1$;

(ii) $f(x)$ is a unit in $\mathcal{R}(\alpha, \beta)$ if and only if $\mu(a_0) \neq 0$.

Proof. Note that we can write x as $x = \alpha_0(\alpha_0^{-1}x - 1) + \alpha_0$ so that $x^i = (\alpha_0(\alpha_0^{-1}x - 1) + \alpha_0)^i$ for $0 \leq i \leq p^s - 1$. Hence $f(x) \in \mathcal{R}(\alpha, \beta)$ can be written as

$$f(x) = a_0 + a_1(\alpha_0^{-1}x - 1) + a_2(\alpha_0^{-1}x - 1)^2 + \cdots + a_{p^s-1}(\alpha_0^{-1}x - 1)^{p^s-1}.$$

Since $a_0 \in R$, it can be written uniquely as $a_0 = \mu(a_0) + a_{0,1}p + \cdots + a_{0,e-1}p^{e-1}$ with $a_{0,i} \in F_{p^r}$. Hence $f(x)$ can be expressed as

$$f(x) = \mu(a_0) + ap + (\alpha_0^{-1}x - 1)g(x),$$

for some $a \in R$ and $g(x) \in \mathcal{R}(\alpha, \beta)$. Define

$$A(x) = f(x) - \mu(a_0).$$

Since $(\alpha_0^{-1}x - 1)$ and p are nilpotent in $\mathcal{R}(\alpha, \beta)$, it follows that ap is nilpotent in $\mathcal{R}(\alpha, \beta)$. Therefore $A(x)$ is nilpotent in $\mathcal{R}(\alpha, \beta)$, so by Lemma 5.1 $f(x)$ is a unit if and only if $\mu(a_0)$ is a unit in F_{p^r} , i.e., $\mu(a_0) \neq 0$. \square

Theorem 5.4 *The ring $\mathcal{R}(\alpha, \beta)$ is a chain ring with maximal ideal $\langle(\alpha_0^{-1}x - 1)\rangle$ with residue field F_{p^r} , and the nilpotency index of $(\alpha_0^{-1}x - 1)$ is ep^s . The ideals of $\mathcal{R}(\alpha, \beta)$ are $\langle(\alpha_0^{-1}x - 1)^i\rangle$, $0 \leq i \leq ep^s$.*

Proof. Let $a(x)$ be an element in $\mathcal{R}(\alpha, \beta)$. Then from Lemma 5.3, $a(x)$ can be expressed as

$$a(x) = a_0 + pa + (\alpha_0^{-1}x - 1)g(x),$$

where $a_0 \in F_{p^r}$, $a \in R$ and $g(x) \in \mathcal{R}(\alpha, \beta)$. If $a_0 = 0$, then $a(x) = pa + (\alpha_0^{-1}x - 1)g(x)$. By Lemma 5.2, $p = (\alpha_0^{-1}x - 1)^{p^s}(\rho(x))^{-1}$, and hence $a(x) = (\alpha_0^{-1}x - 1)h(x)$ for some $h(x)$ in $\mathcal{R}(\alpha, \beta)$. This gives that $a(x) \in \langle(\alpha_0^{-1}x - 1)\rangle$. If $a_0 \neq 0$, then $a(x)$ is a unit in $\mathcal{R}(\alpha, \beta)$. Therefore for any element $a(x) \in \mathcal{R}(\alpha, \beta)$ either $a(x)$ is a unit or $a(x) \in \langle(\alpha_0^{-1}x - 1)\rangle$. This implies that $\mathcal{R}(\alpha, \beta)$ is a local ring with maximum ideal $\langle(\alpha_0^{-1}x - 1)\rangle$. Hence from [15, Proposition 2.1], $\mathcal{R}(\alpha, \beta)$ is a chain ring whose ideals are $\langle(\alpha_0^{-1}x - 1)^i\rangle$, $0 \leq i \leq ep^s$. \square

Corollary 5.5 *There are $1 + ep^s$ $(\alpha + \beta p)$ -constacyclic codes of length p^s over R . They are precisely the ideals $C_i = \langle(\alpha_0^{-1}x - 1)^i\rangle \subset \mathcal{R}(\alpha, \beta)$ for some $0 \leq i \leq ep^s$. Then the number of codewords in C_i is $|C_i| = p^{r(ep^s - i)}$.*

Proof. An $(\alpha + \beta p)$ -constacyclic code of length p^s over R is an ideal of $\mathcal{R}(\alpha, \beta)$. From Theorem 5.4, we have that these ideals are $C_i = \langle(\alpha_0^{-1}x - 1)^i\rangle$ with $0 \leq i \leq ep^s$. Then by Lemma 2.1, we deduce that $|C_i| = p^{r(ep^s - i)}$. \square

Example 5.6 *Let $\mathbb{Z}_9 = \{0, 3, 6\} \cup \{2, 2^2, 2^3, 2^4, 2^5, 2^6\}$ and $n = 3^3$. We have that $(3^3, 6) = 3$ if $\alpha = 2^3$. Let β be a unit in Z_9 . If C is a $(-1 + 3\beta)$ -constacyclic code over Z_9 of length 27, then $C = \langle(-x - 1)^i\rangle$ for some $i \in \{0, 1, \dots, 2 \cdot 3^3\}$, and the number of codewords in C is $|C| = 3^{2 \cdot 27 - i}$.*

References

- [1] T. Abualrub and R. Oehmke, *On the generators of \mathbb{Z}_4 cyclic codes of length 2^e* , IEEE Trans. Inform. Theory, 49(9) 2126–2133, Sept. 2003.
- [2] T. Abualrub, I. Siap, *Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$* , Des. Codes Crypt., 42(3) 273–[287, 2007.
- [3] N. Aydin, I. Siap and D. J. Ray-Chaudhuri, *The structure of 1-generator quasi-twisted codes and new linear codes*, Des. Codes Crypt., 24(3) 313–326, 2001.
- [4] E. Bannai, S. T. Dougherty, M. Harada and M. Oura, *Type II codes, even unimodular lattices and invariant rings*, IEEE Trans. Inform. Theory, 45(4) 1194–1205, May 1999.
- [5] A. Batoul, K. Guenda, and T. A. Gulliver, *On self-dual cyclic codes over finite chain rings*, Available online. Des. Codes Crypt. 2012, DOI: 10.1007/s10623-012-9696-0.
- [6] E. Bearne, M. Greferath, J. Pernas and J. Zembrägel, *Algebraic decoding of negacyclic codes over \mathbb{Z}_4* , Proc. Workshop on Coding and Crypt., 101–110, Apr. 2011.
- [7] T. Blackford, *Cyclic codes over \mathbb{Z}_4 of oddly even length*, Appl. Discr. Math., 128(1) 27–46, May 2003.
- [8] T. Blackford, *Cyclic codes over \mathbb{Z}_4 of even length*, IEEE Trans. Inform. Theory, 49(6) 1417–1424, June 2003.
- [9] A. Bonnecaze, P. Solé, and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory, 41(2) 366–377, Mar. 1995.
- [10] N. Bourbaki, Commutative Algebra, Springer-Verlag, New-York, 1989.
- [11] A. R. Calderbank and N. J. A. Sloane, *Modular and p-adic cyclic codes*, Des. Codes Crypt., 6(1) 21–35, July 1995.
- [12] M. Demazure, *Cours D’Algèbre: Primalité, Divisibilité, Codes*, Cassini, Paris, 1997.
- [13] M. C. V. Amarra and F. R. Nemenzo, *On $(1 - u)$ -cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$* , Appl. Math. Lett., 21(11) 1129–1133, Nov. 2008.
- [14] S.T. Dougherty, T.A. Gulliver and J.N.C. Wong, *Self-dual codes over \mathbb{Z}_8 and \mathbb{Z}_9* , Des. Codes Crypt., 41(3) 235–249, Dec. 2006.
- [15] H. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory, 50(8) 1728–1744, Aug. 2004.

- [16] H. Dinh, *On the linear ordering of some classes of negacyclic and cyclic codes and their distributions*, Finite Fields Appl., 14(1) 22–40, Jan. 2008.
- [17] S. T. Dougherty H. Liu, and Y.H. Park, *Lifted codes over chain rings*, Math. J. Okayama Univ. 53 39–53, Jan. 2010.
- [18] S. T. Dougherty and H.-W. Liu, *Cyclic codes over formal power series*, Acta Math. Scientia, 31B(1) 331–343, Jan. 2011.
- [19] S. T. Dougherty, J. L. Kim and H. Liu, *Construction of self-dual codes over chain rings*, Int. J. Inform. and Coding Theory, 1(2) 171–190, Mar. 2010.
- [20] G. D. Forney, N. J. A. Sloane, and M. Trott, *The Nordstrom-Robinson code is the binary image of the octacode*, in Proc. DIMACS/IEEE Workshop on Coding and Quantization, Calderbank et al., Amer. Math. Soc., 1992.
- [21] M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and Macwilliam’s equivalence theorem*, J. Combin. Theory A, 92(1) 17–28, Oct. 2000.
- [22] K. Guenda and T. A. Gulliver, *MDS and self-dual codes over rings*, Finite Fields Appl., 2012.
- [23] K. Guenda and T. A. Gulliver, *Self-dual repeated root cyclic and negacyclic codes over finite fields*, Proc. IEEE Int. Symp. Inform. Theory, Boston, MA, July 2012.
- [24] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The Z_4 linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, 40(2) 301–319, Mar. 1994.
- [25] T. Honold and A. A. Nechaev, *Weighted modules and representations of codes*, Tech. Univ. München, Fak. Math. Report, Beitrage Zur Geometrie and Algebra, 36, 1998.
- [26] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, New York, 2003.
- [27] F. J. MacWilliams, *Combinatorial Properties of Elementary Abelian Groups*, Ph.D. thesis, Radcliffe College, Cambridge, MA, 1962.
- [28] B. R. McDonald, *Finite Rings with Identity*, Pure and Applied Mathematics, 28, Marcel Dekker, New York, 1974.
- [29] S. Jitman and P. Udomkavanich, *The gray image of codes over finite fields*, Int. J. Contemp. Math. Sci., 5(10) 449–458, 2010.

- [30] P. Kanwar and S. R. López-Permouth, *Cyclic codes over the integers modulo p^m* , Finite Fields Appl, 3(4) 334–352, Oct. 1997.
- [31] S. R. López-Permouth and S. Szabo, *Repeated root cyclic and negacyclic codes over Galois rings*, in Applied Algebra, Algebraic Algorithms and Error-Correctin Codes, Lecture Notes in Computer Science, 5527 219–222, 2009.
- [32] G. H. Norton and A. Sălăgean, *On the structure of linear and cyclic codes over a finite chain ring*, Applic. Algebra Engr. Comm. Comput., 10(6) 489–506, July 2000.
- [33] J. H. van Lint, “Repeated-root cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 343–345, Mar. 1995.
- [34] J. Watada and R. binti abu Bakr, *DNA computing and its applications*, Proc. Int. Conf. on Intelligent System and Applic., 288–294, Nov. 2008.
- [35] J. Wood, *Extension theorems for linear codes over finite rings*, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, T. Mora and H. Matson Eds., Lecture Notes in Computer Science, 1255 329–340, Springer-Verlag, New York, 1997.
- [36] J. Wolfmann, *Negacyclic and cyclic codes over \mathbb{Z}_4* , IEEE Trans. Inform. Theory, 45(7) 2522–2532, Nov. 1999.